Domain Formation and Maintenance in Large Ad hoc Networks[1]

Karthikeyan Chandrashekar
Electrical and Computer Engineering Department
University of Maryland, College Park, MD, 20742

Raquel Morera and Anthony McAuley
Telcordia Technologies
Piscateway, NJ

ABSTRACT

The stability and performance of domains or clusters in MANETs is determined by the election metrics used to generate and maintain these domains. In this paper, we evaluate the performance of the distributed Beacon protocol as the topology changes and as a function of the election metric under various conditions. We propose the "domain age" as the primary election metric to maintain more stable domains than "lowest ID", yet requires no more information be collected. We quantify the increased stability using OPNET simulations. We believe that a combination of domain age, node degree and domain strength will provide the Beacon protocol with the ability to maintain good domains in future battlefield networks.

1. INTRODUCTION

In Future Combat Systems (FCS) the vision is to rapidly deploy and manage large ad hoc networks. A way to manage such networks in a scalable fashion is to form independent (hierarchical) domains [MoreraMcAuley 2002]. Treating a large network as a set of domains can greatly improve network performance for functions such as routing, configuration and security. To rapidly deploy large ad hoc networks and to adapt to network changes, automatic configuration of these domains is needed. Maintaining domain configuration as nodes, routers and servers move is probably one of the biggest challenges [MoreraMcAuley 2002]. [MoreraMcAuley 2003] proposes a simple mechanism to detect domain/network splits and merges based on a beacon protocol. The proposed protocol requires in every domain a node to be responsible for sending periodically a beacon message. This message is sent to all nodes in the domain and becomes the heartbeat of the domain. In this paper we evaluate the performance of the beacon protocol when trying to maintain topological domains. We do not assess the performance of the protocol in terms of the reconfiguration cost (architecture dependent), but in terms of number of domain changes a node experiences and number of reconfigurations imposed on the beacon nodes. Number of domain changes is highly related to reconfiguration cost, as for a given scenario there is a fixed cost associated to a domain change. We differentiate between beacon node changes and regular node changes because we believe the reconfiguration cost is different for these two types of nodes.

2. DOMAIN FORMATION AND MAINTENANCE

In this paper, and for simplicity, domains are created based solely on network connectivity, i.e. all nodes in a connected group belong to the same domain. We use the beacon protocol [MoreraMcAuley 2003] both to form and maintain domains. The beacon protocol operates as follows. Each such group (i.e. network partition) has one domain leader (beacon node). The beacon node periodically advertises its domain and priority to the entire network. Nodes upon hearing the beacons from several domain heads evaluate their associations based on their priorities. A node that is isolated will upon expiry of a timer become a domain head and will form its own domain. Network merges and splits would eventually result in each connected sub-group having just one domain head. This same mechanism determines the beacon nodes at start time. The protocol also allows for a periodic reporting mechanism where the members of a domain send a report to the domain head. To reduce overhead the reporting is evoked less frequently that the beacon advertising. The beacon protocol is simple and achieves the domain formation and maintenance for connectivity based domains.

The domain priority sent in every beacon message can relate to different association functions and policies. Several leader election metrics like lowest ID, node degree, virtual ID, degree of connectivity or connectivity to certain networks have been previously proposed and evaluated in the context of distributed clustering. Their main conclusions are: a) lowest ID is stable but not fair as the node with lowest ID has a higher chance of becoming the leader; b) node degree is fair but can result in oscillations due to link fluctuations. In our case since there is a cost associated with configuration of a domain

[1] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance (CTA) Program, Cooperative Agreement DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE **Domain Formation and Maintenance in Large Ad hoc Networks**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Electrical and Computer Engineering Department University of Maryland, College Park, MD, 20742 ; Telcordia Technologies Piscateway, NJ**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**2**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

we would like the domain leader to continue as the leader as long as possible, thus the age of a domain leader is a direct indication of its stability (isolated leaders have zero age). The node degree of the domain leader and number of members in the domain (beacon strength) are also stability indicators. We introduce an election metric that is a function of the 3-tuple **<beacon_age, beacon_degree, beacon_strength>**.

3. SIMULATION RESULTS

We implemented the Beacon protocol in OPNET 10.0. 100 nodes were randomly placed in an area of 2Km x 2Km. Nodes move according to the billiard mobility model. The node speed was varied from 0 – 30 m/s and the Beacon timer (how often the beacon message is sent) was varied from 5 – 20 seconds. The communication range was 200m, this ensures that the network has sufficient degree of network splits and merges. The greatest ID (GID) metric and the Beacon age (Age) metric were implemented as the association function in the Beacon protocol. We study the domain changes and differentiate between a leader changing domains and a regular member changing domains. Clearly a node becoming a domain head or a domain head becoming an ordinary node will have a higher reconfiguration cost.

Fig 1 shows the per-node number of domain changes for the simulation time (20 min) involving beacon nodes as a function of the node speed and the beacon timer. Clearly the number of domain changes decreases as the Beacon timer increases, this is due to the fact that with a higher Beacon timer, Beacon advertisements are less frequent. We also see that for all Beacon timer values the GID algorithm has more beacon changes than the Age metric with the difference growing as the speed increases. This is because the Age metric is less susceptible to micro mobility and also that an isolated node joining a group can never become a domain leader. Hence using the Age metric will result in fewer reconfigurations involving domain leaders.

Fig 2 shows the domain changes involving non-leader nodes. Interestingly, we find that there are more domain changes for the Age metric than the GID metric. This implies an increased node reconfiguration cost. However, since leader reconfigurations are more costly the Age metric would result in lesser total reconfiguration cost.

We have also obtained the cumulative distribution function of the duration for which nodes remain part of the same domain. The 90% percentile for beacon frequencies of (5s, 10s, 15s, and 20s) is (20s, 40s, 45s, and 80s) respectively for a speed of 10 m/s. We observe that the higher the beacon timer, the larger the affiliation duration for node. This is due to the fact that a node may be disconnected, for a short elapse of time, from its domain and reconnect back to the same domain. Larger beacon timers would not be able to catch this effect, while lower beacon timers do capture this effect and would show at least two more reconfigurations.

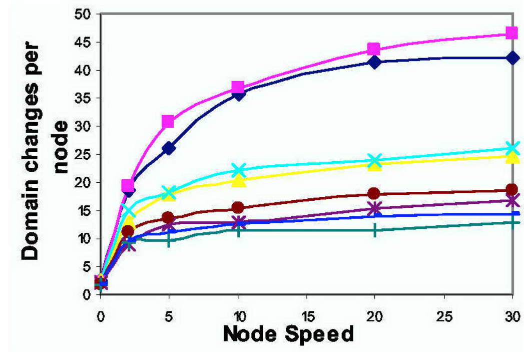

Fig 1: Domain changes involving leader nodes

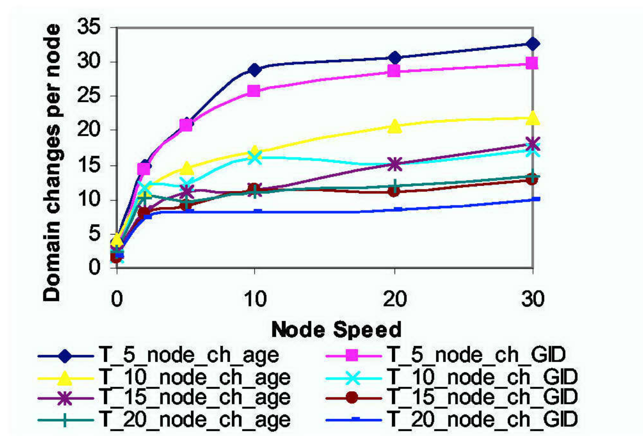

Fig 2: Domain changes involving non-leader nodes

CONCLUSION[i]

The "domain age" is proposed as a new election metric for domain formation and maintenance protocols (Beacon). Experiments show that using the domain age metric results in stable domains compared to the Lowest ID metric. We see that the domain age metric reduces domain leader changes and hence reduces reconfiguration cost compared to the Lowest ID metric.

REFERENCES

R. Morera and A. McAuley, "Flexible Autoconfigured Domains for more Scalable, Efficient and Robust Battlefield Networks", IEEE MILCOM OCT 2002

R. Morera, McAuley et al, "Robust Router Reconfiguration in Large Dynamic Networks". IEEE MILCOM, OCT 2003

[i] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government